UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

WIKIMEDIA FOUNDATION, et al,	:	Civil Action No
Plaintiffs,	:	
versus	:	1:15-CV-662
NATIONAL SECURITY AGENCY/ CENTRAL SECURITY SERVICES, et al,	:	
Defendants.	:	May 30, 2019

The above-entitled Remand Hearing was heard by the Honorable T.S. Ellis, III, United States District Judge.

A P P E A R A N C E S

FOR THE PLAINTIFF:
PATRICK TOOMEY, ESQ.
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004

ALEX ABDO, ESQ.
ASMA PERACHA, ESQ.
Knight First Amendment Institute at Columbia University
475 Riverside Drive Street
Suite 302
New York, NY 10115

FOR THE DEFENDANTS:
OLIVIA H. SCOTT, DOJ
RODNEY PATTON, DOJ
JAMES GILLIGAN, DOJ
JULIA BERMAN, DOJ
U.S. Department of Justice
Civil Division, Federal Programs Branch
1100 L. Street, N.W., Room 11200
Washington, D.C. 20005

OFFICIAL COURT REPORTER: MS. TONIA M. HARRIS, RPR
United States District Court
Eastern District of Virginia
401 Courthouse Square, Ninth Floor
Alexandria, VA 22314

P R O C E E D I N G S

(Court proceedings commenced at 2:42 p.m.)

THE DEPUTY CLERK: The Court calls civil case Wikimedia Foundation versus National Security Agency, et al. Case No. 2015-CV-662.

May I have appearances, please. First, for the plaintiff.

THE COURT: All right. Who is here on behalf of Wikimedia?

MR. TOOMEY: I'm Patrick Toomey on behalf of Wikimedia Foundation.

THE COURT: All right. Anybody with you today, Mr. Toomey?

MR. TOOMEY: Yes. With me are Asma Peracha and Alex Abdo from Knight First Amendment Institute.

THE COURT: Well, the only defendant [sic] remaining is Wikimedia. I take it the remaining attorneys are here to support you.

MR. TOOMEY: That's correct, Your Honor. Thank you.

THE COURT: Good afternoon to all of you.

Now, who is here on behalf of the Government?

MS. SCOTT: Yes, Your Honor. I'm Olivia Hussey Scott or Ms. Scott. Scott is fine. I'm here on behalf of the Government defendants along with my co-counsel, Jim Gilligan, Rodney Patton, and Julia Berman.

THE COURT: And who will argue today on behalf of the Government?

MS. SCOTT: I will, Your Honor.

THE COURT: Good afternoon to all of you.

All right. This matter is here on remand. I granted in part, I granted a motion to dismiss on standing grounds. The Fourth Circuit affirmed in part and remanded in part leaving only one defendant. I'd forgotten how many there were that are no longer here that I dismissed. So we're really here today to consider whether, on this summary judgment record, because I allowed modest or partial discovery on the issue of standing, some questions that were asked, were not answered because the Government invoked the state secrets privilege, and there is some argument about that that I will hear today. But I won't hear any state secrets today. I think that's clear. Nothing classified has been submitted or reviewed by the Court in connection with this. Nothing has been reviewed in camera or ex parte.

Let's begin, Ms. Scott, with you. You're the movant. Put me in the picture, if you will, I think your task today is to persuade the Court that the summary judgment record, as it exists, discloses no disputed material issue of fact on the existence or in your view, lack of existence of injury in fact to the plaintiff.

Do I have that about right?

MS. SCOTT: You do, Your Honor, yes. That is the first part of my argument and the Court also referenced the state secrets privilege related part.

THE COURT: All right. Go ahead. I'll hear from you. And if I remain standing it's for the comfort of my back, no other purpose.

MS. SCOTT: Okay. Well, the plaintiff, as we said in our papers, the plaintiff has no competent evidence in support of two of the three key allegations that the Fourth Circuit found would, if proven, support their standing. And without competent evidence of both of those two key facts, this case must be dismissed.

And first, they have no proof sufficient for a genuine issue of material fact that Upstream surveillance is conducted on what they allege are international Internet links. They rely really on a single sentence from an 80-page FISC opinion, and which is inadmissible for factual matters and doesn't say what they claim it says. I'll talk about that in a little bit more.

Second, they also have no proof sufficient for a genuine issue of material fact that, as a matter of technological necessity, the NSA must be copying all or nearly all communications transiting any monitored link. And there is no factual dispute here. In fact, the undisputed evidence shows the opposite of what plaintiffs were originally arguing

in this case. Plaintiff's own expert admits that Upstream's surveillance program could be operated in multiple ways.

THE COURT: Before you continue, just enlighten us all with what you mean by "Upstream surveillance."

MS. SCOTT: Yes, Your Honor. Upstream surveillance is authorized under Section 702 of the Foreign Surveillance -- Foreign Intelligence Surveillance Act.

Under Section 702, there are two types of surveillance. Colloquially --

THE COURT: I wanted to know what "Upstream surveillance" means.

MS. SCOTT: Yes, Your Honor. So as technically -- well, Upstream surveillance is a colloquial term given to the type of surveillance under Section 702 that is operated on the Internet backbone, which are the major trunk lines between providers that operate the Internet.

So Upstream surveillance involves the eventual collection of communications from the Internet backbone. And it's distinct from another program that is also operated under Section 702.

Now, here the reason there's no factual dispute about how Upstream could, as a matter of technological necessity operate, is because both experts agree that Upstream surveillance could be operated either using a copy-all approach, which is described in plaintiff's allegations. That

approach is described in our briefs as a "copy all, then scan." And it involves essentially putting an optical splitter or something akin to that, along the Internet backbone and making a full copy of the entire stream of communications. As alleged by plaintiff.

The experts both agree it could be done that way or it could be done via what's referred -- what I'll refer to here as a "filter first architecture." In the papers that's called a filter, then copy and scan.

It's also called mirroring, as a technical matter, that's the term you might see in Dr. Schulzrinne's declaration. As the experts both say, "filter first," that type of an architecture could be implemented multiple ways.

So here there's no factual dispute as to the fact it can be done multiple ways. And neither expert, not Mr. Bradner, the plaintiff's technical expert, or Dr. Schulzrinne, our technical expert, neither one of them had access to any classified information. So these experts, to the extent they agree that it could be done multiple ways, they are talking about entirely unclassified information.

The only dispute here is about whether there is a technical basis for Mr. Bradner's opinion or if his opinion about how it's most likely done, that's what he offers an opinion on, is actually straying outside of his expertise into conjecture about matters within which he doesn't himself know,

which is the NSA's Court authorized surveillance practices.

Their priorities and practices, their resources, capabilities, and numbers, nature and other things about targets.

He speculates about all of those things and all of those things, as Dr. Schulzrinne explains, are not technical bases for his conclusion, they are his guesses, essentially about what the NSA might choose in order to run Upstream surveillance.

They make the argument that the choices that Mr. Bradner thinks the NSA is making are most likely largely based on incidental reports -- incidental remarks, I apologize, found in a PCLOB report. So the PCLOB is the Privacy and Civil Liberties Oversight Board. It's not the NSA. But plaintiffs, they did do a review and they did issue a report. And they said a few incidental remarks about how NSA's Upstream program is designed or has the goal to be comprehensive and reliable.

THE COURT: Who are these people again?

MS. SCOTT: The PCLOB. I'm using a shortened abbreviation, but PCLOB is Privacy and Civil Liberties Oversight Board.

THE COURT: All right. Go on.

MS. SCOTT: So plaintiff, however, has already used these statements, these remarks about comprehensive and

reliable goals. And in their, now dismissed, dragnet claim. And the Fourth Circuit held that even accepting as true the allegation about what the NSA is incentivized to do, that fact without more doesn't establish a dragnet.

And that's still true here, these PCLOB statements about the goals and what the NSA might be incentivized to do, are not a basis for any technical conclusions about the operation of Upstream. And especially where, as Dr. Schulzrinne explains, that this comprehensive goal could be accomplished in a "copy all" or a "filter first" architecture.

And there are many practical realities he explains undercut the idea that it might be a copy-all.

Even if -- this is the second part of the argument the Court referenced a few moments ago -- even if, however, Plaintiff could raise a genuine issue of material fact as to its standing, this case must be dismissed under the state secrets doctrine because the entire aim of a trial on standing, would be to prove the existence of a state secret privileged fact.

Whether Wikimedia's communications are subject to Upstream, it also -- a trial on standing would also involve indirect facts that are protected by the state secrets privilege, including what method Upstream actually employs and where it is located in order to conduct its operations.

This Court's August 2018 ruling on the motion to compel and Government's assertion of privilege in fact has already held that information to be protected by the state secret doctrine.

Finally, without proof of that copying and scan, the additional arguments the plaintiff raises must fail. And as this Court is aware, *Clapper v. Amnesty International* is a Supreme Court case that is very analogous to the circumstances here. And it directs that any alleged chill in readership or protected measures taken, because of fears of surveillance, without evidence of actual or certainly impending surveillance, are insufficient as a matter of law.

So here, the additional claim -- the additional claims of harm, must fail as a matter of law. And in total, plaintiff has offered no legally cognizable basis to proceed.

Fundamentally, there are three pieces of evidence at the core of plaintiff's arguments. The PCLOB report, which I already discussed a bit, an October 2011 FISC opinion specifically within that large opinion single sentence and then declarations filed by their technical expert, Mr. Bradner.

I'll talk about each of those three types of evidence for each of the two key allegations next.

So first, their allegation that I'll refer to here has kind led to or their second key allegation, that Upstream

occurs at so-called international Internet links. That's what they allege.

First, they rely on the single sentence from an October 2011 FISC opinion. But factual matters, in judicial opinions, are inadmissible hearsay. And that sentence is -- it doesn't say what plaintiffs allege it says. So I'll start with the second of those. The sentence actually says, "The Government readily concedes that the NSA will acquire a wholly domestic 'about' communication if the transaction containing the communication is routed through an international Internet link being monitored by the NSA, or is routed through a foreign server."

Now, this is not --

THE COURT: You just read that. But -- and I have some understanding.

Would you read it, once again, it says: The Government readily concedes, what?

MS. SCOTT: "The NSA will acquire a wholly domestic about communication, if the transaction containing the communication is routed through an international Internet link, being monitored by the NSA, or is routed through a foreign server."

Now --

THE COURT: "Wholly domestic 'about' communication."

What does that mean?

MS. SCOTT: Yes. A wholly domestic communication is a communication where both ends, the sender and the recipient, are U.S. persons. Are reasonably located in the United States.

THE COURT: All right. Go on.

MS. SCOTT: And "about" for the Court's -- the second part of that thing is it's a wholly domestic about and about is a communication type where a selector in the Upstream process that falls after any filtering, the communication is scanned for selectors. And an about selector is one that's not in the to/from, it's within the communication itself.

So that's what it means when it says a "wholly domestic 'about'," it's that type of communication.

The sentence itself is not a statement of fact. It's a hypothetical, an if-then hypothetical. X happens if Y and Z, but, you know, no X if not Y and -- or not Z.

Now, plaintiffs have tried to pull more from this exact sentence than it could be pulled before. Specifically, in their motion to compel, they argued, and the Court rejected, the argument that this sentence constituted an official acknowledgment of monitoring international Internet links.

The Court held that nothing in this statement confirms that the NSA is monitoring multiple Internet links and plaintiff's argument fails because although the Government

has declassified certain information about Upstream, the Government has not yet released the precise information at issue here.

The same thing is true now whether or not Upstream occurs at any international Internet link is protected state secrets privileged information.

It falls under the locations category that the Court has already held as protected, but also the scope and scale and the operational details, all from this Court's order last August.

Now, I'd like to -- so the sentence doesn't actually say what they claim it says. It's a hypothetical within the FISC opinion and it shouldn't be taken as a Statement of Fact. But to the extent they are arguing it is a Statement of Fact, it is inadmissible, because Statements of Fact that are in judicial opinions are inadmissible hearsay. And it does not meet the public records exception for that hearsay rule, because the FISC is an Article III court not part of the executive branch and judicial investigations do not qualify for that exception.

THE COURT: What about the argument that it's an admission of the party?

MS. SCOTT: They do argue that it has been adopted by the NSA, because in the NSA's 30(b)(6) deposition, where the deponent was Ms. Rebecca Richards, she said that the

sentence was accurate as of October 2011, when the order was issued. That is not an adoption here, a plaintiff's interpretation of the sentence. The sentence was accurate. That's what she said. And to the extent that's what they're arguing, that's as far as it goes, because in that same deposition Ms. Richards said, when asked many different ways, if the sentence meant what plaintiff's are claiming -- plaintiff claims it means, which is that Upstream occurs at so-called international Internet links, every time that question was asked, the witness said the privilege was asserted actually by the NSA, and the witness was directed not to answer and the witness in fact followed that instruction because of the privilege.

And again --

THE COURT: And that's reflected not in the FISC opinion, but it would be reflected in the record, is that what you're saying?

MS. SCOTT: Correct.

THE COURT: If we want to see that, where do we look on this record?

MS. SCOTT: Yes, the deposition of Rebecca Richards is plaintiff's exhibit. And I have the exhibit number, but I don't have it -- hold on. I can pull the exhibit number.

THE COURT: Well, it's in that deposition. You don't have page numbers with you today?

MS. SCOTT: I do, Your Honor. If you'd like the specific page numbers I do.

THE COURT: And these would be page numbers in which that specific question was asked and a negative answer was given? Is that what you're saying?

MS. SCOTT: Yes. And I can walk you through that if you'd like.

The deposition of Ms. Rebecca Richards is plaintiff's exhibit -- I apologize, Your Honor. Oh, you know what, it's in the Bradner attachment.

THE COURT: It's in what?

MS. SCOTT: It's attached to their expert's, their technical expert's appendix. And it's Appendix K.

So there we go. So --

THE COURT: You're being handed something by your co-counsel.

MR. GILLIGAN: Thank you, Your Honor.

MS. SCOTT: Thank you. So the transcript of the deposition of Ms. Richards is Appendix K to the declaration of Scott Bradner. Mr. Bradner's declaration can be found at Document 168- -- let me make sure I'll give you the exact --

Okay. Ms. Richard's deposition transcript can be found at Document 168-4, starting at page 105 in the record.

And then specifically within that deposition, she was asked first:

"Is the sentence true?"

And she said: "Yes, that sentence is accurate."

That can be found on page 160, lines 4 to 17.

Then she was asked:

"What do you understand the FISC --"

That's the Foreign Intelligence Surveillance Court.

"-- to mean in its use of the term 'international Internet link' in that sentence?"

The counsel objected and asserted the state secrets privilege, directed her not to answer. And she said:

"I have an unclassified response, at least in part, NSA. So unlike the other words that you had me go through, in terms of definitions that were Telecom providers, you know, sort of --

(Court reporter interruption.)

MS. SCOTT: I apologize. I went too fast. I apologize. Okay.

-- definitions that were Telecom provider, you know, sort of generally what a teleco expert would be, NSA has an understanding of this term that is specific to how Judge Bates described it. But it's classified to provide any further information."

And then she did not provide any further information in response to that question.

That's at page 160, lines 19 through 161.

(A pause in the proceedings.)

MS. SCOTT: Sorry. He's -- he was referring me to page 189 in the brief. That's actually what we cite in our brief. But I'm walking the Court through the fact that the question was asked many different ways.

THE COURT: Yes. I want you to finish.

MS. SCOTT: Yes, okay. So then page 163 the Court asked -- or sorry, the questioner asked.

"Is there anything you can tell us unclassified about the nature of the..."

I'm sorry. I skipped ahead, Your Honor. Strike that. I'd like to go back a little.

Page 162.

"Is the NSA's understanding of the term different from the general meaning of the term you described in response to an earlier question as the link between two countries?"

"Objection, calls for the state secrets privilege."

She followed the instruction.

Later on that same page.

"Is your understanding that in using the term "international Internet link" the FISC meant an Internet link that terminates in a foreign country?"

"Objection."

Same objection. Same instruction. She followed the instruction.

The next page of the deposition, 163.

"Is it your understanding that an international Internet link is an Internet backbone circuit with one end in the United States and the other end in a foreign country?"

Same objection, same instruction. She followed the instruction.

As you go through the transcript, Your Honor, you'll see that this was asked in many different ways.

And then on pages 188 and 189, they get to the end of the -- the back and forth, and the question was asked again.

She said, "would you like me to restate the unclassified response?"

"I think you already did answer the sentence as written is true as of October 3, 2011."

And she says, "Yes, the sentence is accurate as of October 3, 2011."

So again, she has said the sentence is accurate, but then she refused to answer any further specific questions about the sentence's meaning, the FISC's understanding of what the sentence meant, and what the Government understood the sentence to mean.

The witness, as we said in our brief, the witness repeatedly refused to state whether the NSA actually monitors such links based on the state secrets privilege.

And the page reference that we put in the brief is actually the broader one. 180 to 189.

So she has specifically -- so the deposition transcript makes clear that although the sentence is accurate, and accurate as of October 3, 2011, that's still true, as I stand here now, as of that date. I can tell you that. But anything further about this sentence and the hypothetical that it presents is classified state secrets privileged information.

THE COURT: Why isn't that sentence enough to carry the plaintiff's where they want to go?

MS. SCOTT: Because the sentence does not -- as a hypothetical, the sentence doesn't actually say that the NSA is monitoring any international Internet links. It says that the NSA will acquire a certain type of communication if the transaction containing the communication is routed through an international Internet link. The second part of that is being monitored by the NSA. So it doesn't say whether or not that is true.

And the plaintiff specifically moves to compel that information. And the Court's order in August of 2018 upheld that that sentence, and specifically in the motion to compel argument, they were arguing that the sentence was the Government's acknowledgment of multiple links because there's a -- oh, I apologize, Your Honor. Specifically, in the motion

to compel argument, they were arguing that -- they were arguing that they wanted to compel specific information about documents defining key terms. That the Government and the FISC have used to describe the operation of Upstream surveillance to the public. And they gave an example, which is specifically this sentence. And they said because the term, "international Internet link" describes the point at which the NSA is monitoring communications on the Internet backbone, they've asked us, you know, they propounded an interrogatory saying give us your understanding of that term.

And the Court held that that term was protected. The understanding of that term and what it means that the further state secrets privilege information was protected. It's protected both as a location, where is Upstream operated. Is it on international Internet links or some other part of the Internet backbone or not.

The intelligence community has publicly acknowledged that the NSA is monitoring at least one circuit carrying international Internet communications, but that that does not mean that the Upstream is operated as the so-called international Internet links.

The breadth of the Internet backbone that is carrying international Internet communications is much larger than just these international Internet links that they have alleged.

So this sentence, you know, this sixth sentence does not -- fundamentally, it does not say what they want it to say. And also, to the extent it is a Statement of Fact, in a judicial opinion, it is inadmissible hearsay, and should be kept out. And Ms. Richards, in fact, did not adopt their interpretation of the sentence.

Admissibility matters here. Plaintiff argues in their papers that admissibility doesn't really matter because their expert can consider hearsay information. But the Supreme Court has made clear that experts cannot rely as a foundational part of their opinion on inadmissible matters.

Specifically, in *Williams v. Illinois*, the Supreme Court said, "If plaintiff cannot muster any independent admissible evidence to prove the foundational facts that are essential to the relevance of the expert's testimony, then the expert's testimony cannot be given any weight by the trier of fact."

Plaintiff also cites the PCLOB report that I mentioned a few moments ago. For support for this part of their allegation, that Upstream occurs on so-called international Internet links, but the PCLOB report says only that Upstream is on circuits facilitating the flow of communications between communications service providers.

And that is not necessarily these international Internet links. So the PCLOB does not support this allegation

of theirs.

The third core piece of evidence that they cite, are the declarations by Mr. Bradner, plaintiff's Internet technology expert.

All of Mr. Bradner's testimony concluding that the NSA monitors these so-called international Internet links comes from his speculation about vague statements in Government decisions. In Government documents, I mean. They're not based on his expertise and so they're not admissible under Rule 702 or *Daubert*.

The NSA's intelligence mission is not a matter within his field of expertise. He testifies in his declarations that he thinks it's logical and unsurprising if the NSA were to be monitoring at least one international Internet link, but you know the fact that the NSA -- the fact that everyone thinks the NSA is on a particular link, or a particular point, might even be a reason that the NSA would choose not to be at that particular point.

Mr. Bradner, at bottom, really, Mr. Bradner may know the technical reasons why someone might want to be at a particular place on the Internet backbone to get a certain type of communication, but he does not know the foreign intelligence reasons or concerns that are at play, or the resource and capability issues that might be relevant to the NSA's decision making.

Now, even if it were admissible, his declarations on this conjecture were admissible, they would be legally insufficient as a matter of law to support their standing, because *Amnesty International* directs that such speculation cannot support standing as a matter of law.

THE COURT: What is it that directs that?

MS. SCOTT: Amnesty -- I'm sorry, *Clapper v. Amnesty International*. Which I refer to --

THE COURT: The Supreme Court's case.

MS. SCOTT: Yes, exactly the Supreme Court's case.

THE COURT: It's better to refer to it as the *Clapper* decision.

MS. SCOTT: I will do so from now on in this argument, Your Honor. Sometimes we refer to it by the non-Government party to make it a littler clearer, because there's multiple cases with the *Clapper* name, but I'll say *Clapper*.

THE COURT: All right.

MS. SCOTT: So you know the FISC opinion, the PCLOB report, nor Mr. Bradner's declarations show or provide sufficient evidence to create a genuine issue of material fact here that the NSA is monitoring with Upstream surveillance international Internet links. And without unclassified evidence showing this, this allegation, like two of the three-legged stool or the second key allegation, cannot be

sustained and their case must be dismissed on that point alone.

The third key -- the third key allegation, is that Upstream must be, or now they're arguing, most likely is done via a copy-all infrastructure. And they based this on, again, these three types of evidence. The first one is the PCLOB report. Again, I have already mentioned that the PCLOB have some incidental remarks about the NSA's goals being to do comprehensive and reliable collection.

But as I said, the Fourth Circuit has already held that statements about what the NSA is incentivized to do in the PCLOB, cannot be a basis for any technical conclusions about the actual operation of Upstream.

That's in line with another D.C. circuit case holding in *Obama v. Klayman* that rejects the district court's inference of standing based on the Government's efforts to create a comprehensive phone record metadata database. And specifically there, Judge Williams pointed out that there are various competing interests that may constrain the Government's pursuit of effective surveillance. And it is possible that these factors have operated to hamper the breadth of the NSA's collection, including, you know, these can be legal, technical, budget funding, other types of collateral concerns Judge Williams pointed to.

And that makes sense because the plaintiff and

Mr. Bradner are really guessing about the meaning of these qualitative and aspirational terms and whether the NSA achieved their goals.

As Dr. Schulzrinne, his declarations point out, there are many practical realities and tradeoffs that cut against those goals. And Mr. Bradner doesn't disagree with that. He just disregards it.

But the PCLOB, plaintiff's evidence, the PCLOB supports Dr. Schulzrinne view. Specifically at page 120. It says that, "Whereas PRISM collection..."

That's the other type of Section 702 surveillance.

"Whereas PRISM collection, as the comparatively simple process, the Upstream process is more complex depending upon the use of collection devices with technological limitations that significantly affect the scope of collection."

Dr. Schulzrinne also points out that the filter first architecture -- which by the way can be implemented in a variety of ways that Dr. Schulzrinne explains -- can achieve this comprehensive level of collection that the PCLOB says is the NSA's goal.

And finally, on this point, I will say that even if in 2014 when this PCLOB report came out, even if Upstream collection was as comprehensive as Mr. Bradner thinks it was, which again, there's no support to make that conclusion, one

way or the other. That's not necessarily true now.

The Internet has grown a lot. There's increased incentive to filter communications since 2014. And the PCLOB report itself talked about how at the time the NSA couldn't stop what the court -- what we talked about a moment ago, which is the "abouts" type of communications collection -- without harming the main focus of the program, which is the to/from collection.

So the PCLOB says, "They can't stop abouts without harming the to/from collection." But plaintiff's evidence, specifically exhibit -- their Exhibit 45, is NSA's statement, public statement, about stopping abouts collection. And that happened in early 2017. Page 2 to 3 of that exhibit says that nothing has changed from the PCLOB statement, but nonetheless, the NSA has decided to stop abouts.

So although we can't specifically say what has changed, the evidence that even plaintiff puts forward shows that something has changed.

Now, they also put forward the same FISC opinion, the same sentence within the FISC opinion, for this leg 3 or third allegation that Upstream must be or most likely is done via a copy-all architecture.

And at first, as I've already said, judicial opinions, the statements of fact within judicial opinions, are not admissible for the same reasons I've already given the

Court, this sentence is not admissible.

But second, just as before, the sentence does not actually support their copy-all contention or conclusion. You know reading it again, the sentence says, "The NSA will acquire a wholly domestic 'about' communication, if the transaction containing the communication is routed through an international Internet link being monitored by the NSA."

Plaintiff argues that this sentence must mean the NSA is not using IP filtering.

THE COURT: Is not using what?

MS. SCOTT: An IP filter.

THE COURT: All right.

MS. SCOTT: That's an Internet protocol filter. It's a specific type of filtering. Because if they used an IP filter, it would eliminate the wholly domestic transaction before copying. And the NSA would never collect the transaction between U.S. IP addresses. And they make that argument in their first brief.

Dr. Schulzrinne points out that that's actually not technically correct, because passing all transactions through an IP filter to eliminate wholly domestic transactions could still result in the theoretical acquisition of a wholly domestic communication as described in the FISC hypothetical.

And then, Mr. Bradner does not respond to that technical correction.

Their remaining textual argument about this sentence is that the "will acquire" language there, must mean will acquire all. Now the word "all," is not in the sentence. It says "will acquire a." And so it plainly doesn't say that. And it's also still, it's a hypothetical. So it's not a statement of fact. I've already said that.

But moreover, reading the word "all," the way they do for this argument, into this sentence, ignores the context within which that sentence appears in the FISC opinion. Specifically, the FISC in this part of its opinion is discussing the NSA's technical means. It's not discussing the scope or scale of collection. And it's talking about the NSA's technical inability to prevent the acquisition of wholly domestic communications under certain circumstances. And the FISC finding is the acquisitions occur by normal operation and not as a result of a technical failure or malfunction of equipment.

So reading "all," the word "all" into this sentence, converts it from a hypothetical about the technical operation into a hypothetical about the scope or scale of collection, which is not -- it doesn't contextually fit within what the FISC is actually saying.

Moreover, Mr. B's interpretation ignores that the FISC, in an earlier section, specifically at page 36 of this exhibit, Plaintiff's Exhibit 16, note 34. There, the FISC is

discussing the same phenomenon. This inability to prevent the acquisition of some wholly domestic communications, and there the FISC observes that the NSA may acquire wholly domestic communications, not that it will acquire all of them.

You know, this interpretation of Mr. Bradner is a good example of him straying beyond his expertise to interpret a judicial opinion in one way or the other. And the Court does not need his assistance in order to interpret a judicial opinion.

Finally, same as what we talked about a moment ago with the PCLOB, even if -- even if Upstream operated, as plaintiff's allege, which again we say there is not proof sufficient for a genuine issue of material fact to support their allegations. But even if it operated at the level that they claim it did in 2011, there's no evidence that operations today are the same as they were in 2011.

Just as before, when I mentioned, there's been an enormous growth of the Internet, additional incentives to filter, and the Government is no longer, since early 2017, getting abouts collection, which does impact the scope of collection.

Now, the third category of evidence that they rely on for this argument that Upstream must be or most likely is done via copy all, are the declarations filed by their technical expert, Mr. Bradner. As I've already said, he

admits that it can be technically possible to use either a copy all or a filtering, one of the many ways of filtering process, in order to operate Upstream collection.

From there, as I've said, he strays beyond his experience into matters of court authorized surveillance and foreign intelligence questions.

I can provide the Court with some examples of this straying. Specifically, he claims that copy first is more likely than the filter first, because the NSA is unlikely to share sensitive information about its targets and/or filtering criteria within an assisting provider.

This is guessing about the NSA's willingness to share classified information with a provider. It's not a technical basis for a conclusion. Plus it's an iffy premise. The NSA already shares sensitive information with the provider in some instances. The PCLOB report the plaintiff attaches evidence, identifies that this happens, for example, with selectors like e-mail addresses.

Mr. Bradner also claims, as an example, that copy first is more likely, because it requires no placement of an NSA operated device into the heart of a provider's network. But as Dr. Schulzrinne's points out, neither would the filter first architecture that he's proposing, the filtering method that he said is technically available as an alternative, would be low risk.

Specifically, it is operated, the filter first architecture that Dr. Schulzrinne proposes, is operated within the provider's own routers and switches.

So to back up for a moment, the routers and switches are the points where, as the light streams or the electronic data is moving through the Internet backbone, the normal operation of the router or the switch is to receive that transmission, decode it, and examine the header information to decide where to send it onto next, along the Internet backbone. Or if it's going to come off the backbone into a more -- a -- as it travels closer to the user, the end destination.

So as part of their normal operations, these routers and switches decode the information, look at the IP address header, the header information, and then they send it on to their next destination.

As part of the providers' normal operation, Dr. Schulzrinne explains, the providers do filtering themselves. And this filtering is called mirroring also, where they do it for their own network security, for their own network maintenance reasons, they also do it to try and stop denial of service attacks or other malicious attacks on their system. So what's done in that process is the router, when it decodes the information and looks at the IP -- the header information, it then compares that header information against

what's called an "access control lists." Those access control lists are loaded with information. Should this, you know, that describes is something to be whitelisted or blacklisted, or filtered as the provider wants it to be. And if it's a communication that has been whitelisted, meaning the provider wants to look at this type of communication or the communication itself for some reason, for its own business purposes, it would mirror the communication or make a copy before it goes on its way.

Now, this process is happening at -- in nanoseconds. So faster than I can even say the "c" in copy, it's done. And it's moving at an extremely rapid pace.

The blacklist version of this filtering, is where the access control list is loaded with a don't give me an instruction, don't give me any information -- any communications that meet these qualities.

So this mirroring or filtering process is already running in the provider's own network. And Dr. Schulzrinne explains that the mirroring process could be utilized by providing the provider the information they need, they can load and access control lists and utilize either whitelisting or blacklisting. And again, he is -- he is describing this as a technical alternative, not -- he doesn't have access to classified information so he's not saying how it's actually run. He's saying it's a possibility.

Through blacklisting it or whitelisting, they can either block a communication or send it through to an NSA operated device. They can also use a combination filtering so they could blacklist all types of communications or all communications from a certain IP address, and then only whitelist the ones that are of specific interest as a combination approach.

So this -- what Dr. Schulzrinne is saying is that Mr. Bradner is wrong, that filter first would be riskier because it would require placing a device in the heart of the provider's network that is NSA operated. But that's actually not the case, because as Dr. Schulzrinne proposes it, the provider would use -- the provider would use its own system as it operates in the ordinary course of business.

THE COURT: Well, we've spent a good deal of time here talking about various expert's speculation, speculations as to what might be done, because, as you would remind me, what's actually done is subject to the state secrets privilege. Tell me then, what is the standard that you think the Court must apply to find standard? Must I be persuaded by a preponderance of the evidence that is not disputed that there is injury in fact?

MS. SCOTT: The standard that this Court should apply for standing in this case is the standard -- the same standard that was articulated in the *Clapper v. Amnesty*

International case. The evidence showing injury would have to be showing actual or certainly impending injury.

As the Court in *Clapper* --

THE COURT: Would I have to know what's actually done?

MS. SCOTT: Well, Your Honor, as we've said our position is that they have not proven, using the unclassified evidence, that there is a genuine issue of material fact about whether or not they have standing. They have not shown that they have standing because they cannot show either actual or certainly impending injury. They can't, in fact, show that their communications are --

THE COURT: Well, isn't the only way to show that, to breach the state secrets privilege, and find out what's actually done?

MS. SCOTT: Your Honor, from here, correct. That is the second part of my argument. So because they cannot show a genuine issue of material fact on standing, we think the Court should dismiss on that basis, but the Court also should dismiss, because from this point, even if they could show with unclassified evidence a genuine issue of material fact, at this point, the case would have to be dismissed under the state secrets privilege doctrine. Because, you can't hold a trial on the question of standing where the very question of standing, the outcome of that, is a protected state secrets

privileged fact.

This case in that way is exactly, at this point, like *El-Masri*, where the Fourth Circuit found that for purposes of the analysis, the central facts, or the very subject matter of an action, are the facts that are essential for the claim to proceed or for the -- to prosecuting the action or defending it.

At this point we now know that for them to attempt to prove standing, as they would propose, now we should have a trial on standing, that such a trial can't happen because the whole object would be to prove whether Wikimedia communications are subject to Upstream. And the Court, this Court has already held in August 2018 that such a fact is protected by the state secrets privilege.

A trial on standing would also indirectly bear on other state secrets privileged questions, as we've now seen made plain through the briefing, whether or not the NSA uses a copy all or a filter first or some version of the filter first architecture. That's protected state secrets information because it's operational details. Whether or not Upstream is operated at one or more of these so-called international Internet links, that's also state secrets privileged information. It's locations of Upstream.

So just like in *El-Masri* where the plaintiff argued, well this CIA rendition program has been publicly acknowledged

and so we can go forward, the privilege is undermined. No, this is just like *El-Masri* where the operational details are what is protected by the privilege here.

And because you would have to get into those protected pieces of information in order to have a trial on standing, this case can proceed no further.

THE COURT: All right. Anything further? You'll have an opportunity to respond, but it's -- you've argued for quite a while now, and I think we have a pretty good idea of your position. Is there anything you want to say before I give Mr. Toomey an opportunity?

MS. SCOTT: I will take the Court's guidance, and knowing I will come back and have another opportunity, I will defer at this time.

THE COURT: All right. Mr. Toomey.

MR. TOOMEY: Thank you, Your Honor. And may it please the Court.

For all the bluster in the Government's briefs there's no question that Wikimedia has put forward more than enough evidence to support its standing and defeat summary judgment.

I want to touch on Wikimedia's showing first before addressing why this case can and should proceed in light of the procedures that Congress made mandatory in FISA.

Wikimedia evidence supports each of its three key

allegations. First, Wikimedia's trillions of communications across every international Internet link in and out of the United States.

Second, the NSA is monitoring at least one of these international links.

And third, the NSA cannot conduct Upstream surveillance as it has been described in the Government's own documents without copying and reviewing some of Wikimedia's communications on these links. Wikimedia's expert, Scott Bradner, explains in great detail why these public documents support his conclusions. But the basic idea is not complicated. The NSA's systematic surveillance of Internet traffic invariably touches some of Wikimedia's ubiquitous communications. The Government's expert, Henning Schulzrinne, disagrees with some of Bradner's points. But notably, he does not disagree with Bradner's key conclusion: That the NSA is in fact copying and reviewing some of Wikimedia's communications.

THE COURT: Where does it show that he doesn't disagree with that?

MR. TOOMEY: He never contests Mr. Bradner's conclusion that there is a virtual certainty that the NSA is copying, reviewing some of Wikimedia's communications.

At no point --

THE COURT: Does it say that or is that an inference

you draw from his declaration?

MR. TOOMEY: He never disputes it. He never addresses - -

THE COURT: I'm sorry, answer my question.

Does he say that or is it an inference you're drawing?

MR. TOOMEY: He does not say, "I don't dispute this finding." He says --

THE COURT: All right. Well, that's what I wanted to be clear about because if he did say that, I'd want you to point it to me.

MR. TOOMEY: Understood, Your Honor.

THE COURT: That doesn't mean that your argument that he effectively admits that for the reasons that you state. It doesn't dispose of that argument, but it puts it in the proper light.

MR. TOOMEY: That's right. And of course, the Court is assessing, at this stage of the case, whether plaintiffs have put forward enough evidence to establish a genuine dispute of material fact. So I do want to emphasize that the Court isn't deciding, at this stage of the case, whether Mr. Bradner or Mr. Schulzrinne is correct in any of the statements that they made, but whether there is a genuine dispute as to whether Wikimedia has put forward evidence that would support its showing that there is a substantial

likelihood that its communications are being intercepted.

THE COURT: What evidence, other than what's reflected in your expert's declaration, have you put forward on standing?

MR. TOOMEY: We point to the documents that are discussed in our briefs. Some of which have already been disclosed today. The FISC opinion, the Government's submissions to the FISA court, the report by the Privacy and Civil Liberties Oversight Board, the Government's responses to our discovery requests, the testimony of the NSA's witness at its 30(b)(6) deposition, and a host of documents, many of them are cited in the appendix to Mr. Bradner's opinion.

THE COURT: All right. If I were to proceed to hear this case on the standing issue, which in effect is the merits issue, if I were to proceed to hear the case on the standing issue, wouldn't we have to get into the state secrets privilege that the Government asserts? That is, the material as to which the state secrets privilege has been asserted.

MR. TOOMEY: FISA procedures here provide the Court --

THE COURT: I mean can I get a yes or a no and then you can go on and explain it?

If I go ahead and litigate standing, won't I have to consider matters as to which the Government has asserted the state secrets privilege?

MR. TOOMEY: You might, Your Honor. If the Court were to use FISA's procedures --

THE COURT: Whose procedures?

MR. TOOMEY: The procedures in the Foreign Intelligence Surveillance Act, Your Honor. In Section 1806(f) of the statute.

THE COURT: All right. Go on.

MR. TOOMEY: Congress laid out a set of procedures governing discovery of material related to FISA surveillance.

THE COURT: Is that related at all to CIPA?

MR. TOOMEY: It is a different statute.

THE COURT: I know it's a different statute, but I mean, obviously, that material is classified and CIPA purports to govern all use of classified information in litigation.

MR. TOOMEY: My understanding, Your Honor, is that CIPA governs in criminal proceedings.

THE COURT: You're correct.

MR. TOOMEY: But FISA --

THE COURT: But civil --

MR. TOOMEY: The FISA statute applies in both criminal and civil proceedings, as Congress made clear when it enacted FISA.

THE COURT: That's correct. Go on.

MR. TOOMEY: So in our view, and I want to put this in practical terms, Your Honor, that the way for the Court to

proceed, is Wikimedia has adduced evidence showing that the NSA is copying and reviewing some of its trillions of communications, consistent with the Court's prior ruling on the state secrets issue last August, this showing is sufficient to trigger FISA's in camera review procedures to permit the Court to consider classified evidence in ex parte fashion that addresses this standing issue.

And the -- the Court should use those procedures to review additional evidence that will make this case far simpler. The procedures require the Government to present actual evidence about the surveillance at issue, rather than their outside expert's increasingly elaborate theories about what the NSA might be doing.

The Court can require the NSA to state directly whether it has attempted to filter out every single one of Wikimedia's communications, as Schulzrinne theorizes, and if so, the Court can ask for evidence that the NSA has actually succeeded in those efforts to completely avoid Wikimedia's communications.

And the Court should conduct that in camera review with the help of its own expert or special master. As I believe the Court indicated it has done in other technically complex cases.

THE COURT: I indicated what?

MR. TOOMEY: In a prior status conference that I

believe the Court said in a patent case it had --

THE COURT: Yes, I had --

MR. TOOMEY: -- invited its own expert to help --

THE COURT: Let me be clear about that, because I don't think I was -- I may have been complete, but I don't think I was. I'm at the point now where I reminisce a lot. At my age, you'll do the same. Looking forward is not productive.

Many years ago, I participated, I was on the judicial conference committee of both the umbrella committee for the federal rules and also the appellate rules committee, and others, and I participated in considering the rule of evidence that allows appointment of independent experts. I was opposed to that rule, which I may not have disclosed earlier. I was opposed to it, because I felt, in my experience, that if the Court appoints an independent expert, the fact finder, typically a jury, check out whatever the Court-appointed expert says is going to rule. That's human nature. And I didn't think that was a good way to proceed.

It reminded me of the old patent cases. I've been around so long that I can remember, in the '60s and '70s when most patent cases where two experts swearing at each other and a jury deciding which expert they like without any idea what the patent was about or the boundaries of the monopoly branding.

So I wasn't in favor of it. I lost that argument and I won't surprise you to tell you that I've lost a lot of arguments in the past 50-plus years.

I lost that argument. And I said, in losing it, yes, I can see there might be some cases where I would use an independent expert. I think I posited the safety of drinking water in a community or something like that. But by and large I wasn't really moved by it. Well, along comes a patent case and this patent case involves 20 or 25 transistor circuitry patents. Very good lawyers on both sides. Very good experts on both sides from MIT, Duke, Princeton, other places who were very, very good, and I became concerned, for good reason, that they would blow things past me. So I said: Let's have an independent expert. There were 20-some patents, and so I divided -- I took each patent one at a time. There were five groups of patents and I took the first group of four or five, and the way the thing presented -- oh, the experts had to pick the third expert, they had to agree on it.

All right. So that's how we proceeded. And I heard one expert, and then I heard the other expert, and then I heard the Court-appointed expert. After three patents -- I decided the case after each patent. I decided that patent. After three or four, I don't remember which now, it's been 30 years or so, and I decided it, the parties settled the other 20. And in the course of that, it turned out -- maybe there

were five that I did. But it turned out that I found persuasive the party's experts, one or the other, over the independent expert. I never picked the independent expert. Not because I was biased against an independent expert, but because I concluded that the other was right.

So I guess my view is, I'm not a fan of that rule appointing an independent expert, because I don't farm out decisions, even if they're technically difficult. But, I take your point that I could do that, the rule permits it and I might. I don't cross that bridge until I come to it. But I don't want you assuming that I have some great interest and affection in that. If I can do the problem myself, I'll do it.

MR. TOOMEY: Understood, Your Honor. I think one --

THE COURT: After all, if I can't do it myself, how am I going to judge the validity or the -- the merits of what an independent expert says. I'd end up doing what I've always suspected a jury does in those cases, whatever the independent expert says must be true. Not so.

MR. TOOMEY: I think one additional consideration in this circumstance, and of course it's up to the Court to decide when the time comes, would be that some of these submissions might be in camera submissions. So the Court would be hearing only from the Government. And potentially on quite complex technical questions. And in that posture, it

might be useful for the Court to have --

THE COURT: Yes, I take that point. Go on. That's a valid point. I'll consider that if it comes to that.

MR. TOOMEY: Absolutely.

THE COURT: When we -- if we get to that bridge, I will have to decide and I'll take what you've just said into account. That's a valid point.

MR. TOOMEY: Thank you.

So the Government claims that allowing this case to go any further could reveal sensitive information. But Congress anticipated those claims. FISA's procedures address the Government's concerns by protecting sensitive evidence while explicitly authorizing court review. These procedures are mandatory and the Court should use them just as it has used them in other FISA cases. Especially here where the Government has made extensive public disclosures about the scope and operation of Upstream surveillance and where Wikimedia's trillions of communication can be found on every international link. This would not reveal sensitive information.

Using FISA's procedures here would only confirm what the public record already shows. A ruling that Wikimedia has standing would confirm only that there is a substantial risk that one of Wikimedia's trillions of communications will be copied and reviewed in the course of Upstream surveillance.

Despite the Government's claims the Court need not make any public finding that Wikimedia is or was subject to Upstream surveillance.

THE COURT: Say that again.

MR. TOOMEY: The Court need not make any public finding that Wikimedia is or was subject to the surveillance. The standing threshold is that Wikimedia must show a substantial likelihood.

THE COURT: Well, but -- when we get to the merits, I have to answer that.

MR. TOOMEY: No, I don't believe you do, Your Honor, because Wikimedia is seeking prospective relief, and in order to establish standing for prospective relief it has to show a substantial likelihood that its communications will be intercepted.

THE COURT: So that's really what Wikipedia [sic] has as its first choice. Wikimedia, I mean. All right. Go on.

If this were not a matter subject to state secrets, I'd suggest what an ideal circumstance in which the parties should get together and reach a reasonable solution. But it isn't, because of that factor. Go on, sir.

MR. TOOMEY: Understood.

So as a result a ruling that Wikimedia has standing would not reveal anything more than what the existing record

shows, which is that the NSA is systematically monitoring Internet traffic, including web activity of the kind Wikimedia engages in on a massive scale. Most obviously no target, terrorist, or spy would learn that his or her communications were or were not being surveilled.

Because Wikimedia communicates with hundreds of millions of individuals scattered around the world and because Internet communications take ever-shifting paths, a ruling that Wikimedia simply has standing would reveal no new information about the scope, location, or targets of the surveillance.

THE COURT: And let's assume that we went down that road and that I agreed with everything you did, what is the remedy that you-all seek in this case?

MR. TOOMEY: We're seeking an injunction that -- and a declaratory judgment that the surveillance at issue here, Upstream surveillance, the searching of Internet traffic, in and of out of the United States, violates the Fourth Amendment.

THE COURT: So you would want to stop it.

MR. TOOMEY: That's correct, Your Honor.

THE COURT: All right. Go on.

MR. TOOMEY: Finally, even if the Court believes that some secrecy might be compromised by allowing the case to go forward, that is only because Congress struck a balance in

FISA between secrecy and between the judicial review necessary to ensure that NSA surveillance complies with the law.

So it's not the Court's province to remake the balance that Congress decided on when it enacted FISA and when it provided procedures for the Court to review information, sensitive information in camera.

The Government's argument that FISA's procedures don't apply here is -- are belied by the text, the structure, and the legislative history of FISA.

THE COURT: Sounds like your brief.

MR. TOOMEY: We certainly made some of those arguments in our brief, Your Honor.

But I do want to point out one way in which the Government's arguments interact here, because if the Government could assert the state secrets privilege over whether a party is aggrieved under FISA, which is what it contends here, then no civil case could go forward without the Government's permission.

The remedies that Congress created to impose accountability through the civil remedies in FISA would be illusory. The Government could block any party's, any plaintiff's effort to challenge the lawfulness of surveillance, by claiming that whether or not that party is aggrieved is itself a state secret. It could cut off every case at that juncture.

And because of that, the Government's state secrets claim is incompatible with the FISA statute. The Government has argued that Wikimedia must prove it's aggrieved to invoke FISA's procedures. But in the next bracket says that the state secrets privilege prevents Wikimedia from proving it is aggrieved under the statute. And those arguments would turn FISA's civil remedies into a nullity. No one would be able to avail themselves of those remedies without the Government's permission.

I want to turn now back to Wikimedia's evidence on the summary judgment question. First, I want to emphasize that the Government distorts the summary judgment standard. The Government repeatedly suggests that Wikimedia must prove the copying and review of its communications to a perfect certainty at this stage, but that's a false premise. No other plaintiff would be required to prove its claim to a certainty at summary judgment. And that's not the standard that applies here.

THE COURT: I don't recall that she argued that. My recollection is that she argued that there's not evidence sufficient to establish a material issue of disputed fact.

Am I correct, Ms. Scott?

MS. SCOTT: Yes, Your Honor. That is what I argued.

THE COURT: So there's no point in knocking that straw man down. That's not an argument they make.

MR. TOOMEY: Your Honor, the Government's description of what weight or what implication their expert's declaration has, suggests that Wikimedia can't prove its standing unless it has disproven the hypothetical that Dr. Schulzrinne puts forward.

Their argument is --

THE COURT: No, their argument is that that argument that your expert has put forth is speculative, speculation, and that that's not enough.

MR. TOOMEY: Respectfully, Your Honor, their expert goes beyond that and their arguments go beyond that.

THE COURT: Their expert does. That's how she characterized what your expert says. It's speculation.

MR. TOOMEY: They have certainly argued that our expert is speculating, Your Honor. And we disagree with that. I want to emphasize that Scott Bradner begins with the Government's own official disclosures and he interprets those documents --

THE COURT: Well, let's come to those. Now, let's go directly to those. There were three of those that Ms. Scott mentioned. Why don't you treat each of those.

MR. TOOMEY: Of course, Your Honor.

So the first document is the -- is the FISC opinion, and there, I believe, the Government touched on both the question of whether the surveillance -- there's evidence that

surveillance occurs at international Internet links and then we returned to that -- that same FISC opinion, related to whether the Government is in fact filtering out Wikimedia's communications.

On the question of whether the surveillance occurs at international Internet links, the Government today hasn't disputed that the statement in the FISC opinion is accurate, and its own witness at the 30(b)(6) deposition, at two different places, on page 160 and on page 189, agreed that that statement in the FISC opinion was accurate as of October 2011.

The questioning that occurred -- that the Government read through here, involved questions about going beyond what the statement on the FISC -- in the FISC opinion meant. But, there's no -- there's no genuine dispute that what the FISC said in its opinion is accurate. And that the -- the accuracy of that statement was adopted, at least as of the date of that opinion.

And that should resolve the question whether there's evidence about whether the surveillance occurs at, at least one international Internet link. If the FISC opinion having been adopted is competent evidence of where the surveillance occurs, the Government has not put forward any evidence to the contrary. And that FISC opinion and Government's witness provides sufficient evidence to support plaintiff's showing on

that fact.

We have also discussed the PCLOB report, and, I think, the main focus of the Government's argument has been on the PCLOB's description of Upstream surveillance as being comprehensive. And I have three points that I want to make sure the Court understands.

First, the PCLOB reports discussion of comprehensiveness was not an abstract, hypothetical, or aspirational discussion. I urge the Court to look very closely at the PCLOB report in -- especially that discussion in it, because it makes clear that what the PCLOB was discussing was a very technical description of how Upstream surveillance operates and the technical consequences of the Government's objective of comprehensively collecting communications to and from its targets. In light of the technical constraints that the NSA faces due to the technology it uses to implement Upstream surveillance.

The Government tries to characterize the PCLOB's reference to comprehensiveness as a passing remark, but the PCLOB actually makes that observation at two separate points in the report, including in the executive summary on page 10. So that description is the linchpin of the PCLOB's explanation about why the Government was unable to eliminate about surveillance at that point in time.

And I also want to emphasize that the type -- the

type of comprehensiveness that is being discussed there and that Bradner explains in his opinions is comprehensiveness not in some generalized sense, but on a particular circuit.

The question is whether the NSA is employing any filters to eliminate communications, let alone the types of filters that would completely avoid Wikimedia's communications.

And on that point, the PCLOB report is quite clear, on page 122, that the NSA utilizes and that there exist devices that are capable of examining all the contents passing through collection devices.

And that description in the PCLOB report is consistent with other documents that Bradner points to, including public disclosures in court filings by the British intelligence agencies. And what those documents show is that the British intelligence agency, GCHQ, which is one of the U.S. Government's closest intelligence partners, engages in an analogous form of surveillance that involves copying all the communications on a circuit in order to review them for selectors.

And the reasons that the GCHQ describes in those documents are what it calls: reasons of technical and practical necessity. And those reasons parallel the reasons that Bradner himself describes in his declarations. They include the fact that targets may move from one communications

method to another communications method, that targets are distributed around the globe, and that their communications travel different -- unpredictable paths across the Internet.

And those technical and practical necessities validate Bradner's description of how and why Upstream surveillance is conducted in the way that he says.

Schulzrinne himself acknowledges the feasibility of conducting a surveillance in the way that Bradner describes. He acknowledges that the Government may in fact use a splitter to copy and review all the communications. So neither the PCLOB report, nor Schulzrinne himself demonstrate that the method that Bradner describes is infeasible.

Now, on this -- on this question of whether the NSA employs a secret filter to eliminate Wikimedia's communications entirely. We have also pointed to the FISC opinions description of how wholly domestic about communications are intercepted at international Internet links. And a FISC opinion says that those types of communications will be intercepted at international Internet links. And Scott Bradner explains why that statement would only be true if the Government were not employing filters at those collection points.

The statement -- the statement that the NSA will acquire means that the Government is not employing either the types of filters that would eliminate wholly domestic

communications or the types of filters that Schulzrinne hypothesizes.

And Bradner points to the plain language of that statement in the FISC's own opinion. And the FISC opinion is another document that I hope the Court looks closely at, because it is clear from that discussion that the FISC was not addressing an abstract hypothetical in the way the Government has suggested today or in its papers. The FISC was conducting an extensive investigation into how Upstream surveillance was in fact conducted, because it learned that for years the NSA had misrepresented to the Court how that surveillance actually occurred and the implications that it had for the collection of Americans domestic communications.

The FISC was -- was closely examining the technical methods that the NSA used to screen out communications, and it made statements in reference to the NSA's own submissions. So there was a very good reason for the FISC to be precise and the length and the other sections of its opinion make very clear that it was engaged in a technical discussion of how NSA's surveillance actually occurs.

Between these documents and -- between these documents and Bradner's opinion, there's no question that Wikimedia has put forward evidence supporting its view that at least some of its communications are being intercepted.

Dr. Schulzrinne puts forward a hypothetical about in

his view how the NSA could conduct surveillance without -- without interacting with any of Wikimedia's communication, but he doesn't cite a single document that supports his Wikimedia avoidance theory. He does not cite a single document showing that the NSA is taking any of the steps he theorizes about.

And in fact, he is a vehicle for the Government to put forward the notion that the NSA is employing a secret Wikimedia filter without the Government ever being accountable for the truth of those theories, even in an ex parte submission to the Court.

The Government uses Schulzrinne to put forward a bald hypothetical, one that has no basis in any document in the record. And then, it argues that Wikimedia has to have -- would have to have classified information to disprove that hypothetical. That tactic is not a reason to find Bradner's opinions inadmissible, and it's not a reason to grant summary judgment for the Government.

Bradner has put forward his view not simply that it is most likely that the NSA is copying and reviewing some of Wikimedia's communications, but that it is a virtual certainty, given the technical descriptions of NSA surveillance and the fact that Wikimedia engages in so many communications with so many people around the world.

I want to focus on any questions the Court has if -- if that would be helpful, but unless the Court has -- has

anything further, I do want to emphasize that three factors in this case make it unlike any of the cases that the Government cites in its papers. And some of those factors involve actions by the other branches of Government.

So the first factor is the Government's own disclosures here. The Government made a deliberate decision to provide this information public. It reviewed the FISC opinion in detail and declassified the FISC opinion.

It engaged with the Privacy and Civil Liberties Oversight Board in its investigation into Section 702. It reviewed the report that the Privacy and Civil Liberties Oversight Board produced for both accuracy and classified information. And it has provided a wealth of information to the public for purposes of transparency and accountability about how Upstream surveillance operates.

The second fact is that Congress made a decision in FISA to provide a mechanism that balance the interest in secrecy and accountability. Unlike the state secrets cases that the government points to, including *El-Masri*, Congress provided a mechanism for Courts, like this one, to review classified information in order to hear cases, to hear civil challenges that took on the lawfulness of FISA surveillance.

And so that mechanism, which was a judgment by Congress, is available here. And in fact Congress made -- made it mandatory in cases challenging FISA's surveillance.

And third, plaintiff Wikimedia and its showing are exceptional, because of the size, breadth, and distribution of its communications. Wikimedia engages in so many communications of the kind -- of web communications of the kind the Government has said it's collecting that it can make a showing that few other plaintiffs could.

And together with the Government's own unclassified public disclosures, Wikimedia has provided more than enough evidence to show that its communications are substantially likely to be copied and reviewed in the course of the surveillance.

THE COURT: All right. Thank you.

MR. TOOMEY: Thank you, Your Honor.

THE COURT: Thank you, Mr. Toomey. All right, Ms. Scott.

MS. SCOTT: Yes, Your Honor.

THE COURT: You have the burden of persuasion, so you get the last word.

MS. SCOTT: Yes, Your Honor.

So counsel has just said that there are three factors that make this case different. And the first one that he said is that the Government decided to release information. And so that factor, in making that argument, he forgot to tell the Court that the Court has already ruled that the privilege applies here to the specific information that are operational

details, locations of Upstream surveillance, and the subjects and/or targets. There are other things that the privilege covers, but those are the key things that it covers that are being addressed in their argument.

And this case is *El-Masri* because of that where there had been a general release of information, but not a release of the information that was specifically necessary to litigate that case.

As this Court held and the Fourth Circuit affirmed, the case could not go forward in that circumstance and this case is just like that and it cannot go forward.

The second factor, the 1806(f) can apply. Again, counsel forgot to tell the Court that this Court has already looked specifically at the 1806(f) issue and this Court has already found that 1806(f) does not apply here. Specifically, the August 2018 decision that this Court issued said: That 1806(f) procedures do not apply. I'm going to read directly from the Court's opinion if you don't mind. I didn't want to get it wrong, that's why the pause.

"A determination that surveillance was lawfully authorized and conducted, cannot occur unless a determination has previously been made that the surveillance at issue did in fact occur. Put differently, it is impossible to determine the lawfulness of surveillance if no surveillance has actually occurred. Thus the text of 1806(f) points persuasively to the

conclusion that Congress intended 1806(f) procedures to apply only after it became clear from the factual record that the movant was the subject of electronic surveillance.

Now, here, just like in August of 2018, when the Court made that analysis and issued -- when this Court issued this opinion, plaintiff has failed to prove, on the factual record, that 1806(f) procedures apply. And this Court should not revisit that decision here now. Specifically, they have to prove, as I'll remind the Court you've already decided, that they have -- they qualify as an aggrieved person. And without that aggrieved personhood or aggrieved person status, they cannot get access to those procedures. And the aggrieved person status, in order to prove that, they have got to -- they have got to prove the definition of aggrieved person under 50 U.S.C. 1801, which is the FISA definition for aggrieved person. "Is a person who is subject to electronic surveillance."

And the "electronic surveillance" term that's defined under 1801(f). There are four categories, but all of them require a factual showing of acquisition.

Now, that hasn't been briefed at this stage here, because it is not the same as the standing question. Specifically, neither of the two architectures that are being discussed as the available technical architectures, neither one of them, deal with this question of acquisition. That is

after any filtering stage and it has to do with ingestion into the Government databases.

Now, as I said, we haven't briefed specifically what would an aggrieved person, what would that proof require, because the Court has already held that 1806(f) procedures cannot be used here. They haven't proven they're an aggrieved person. That's the first thing. But also, it would be inappropriate because the statute is aimed, the entire thrust of that statute is aimed at using those procedures to determine the lawfulness of the surveillance, not whether or not surveillance occurred, which is the standing question.

Or that they were subject to surveillance, which is the standing question. So I forgot to tell the Court that it had already ruled and that is directly on point, and Your Honor should not revisit that decision.

THE COURT: Do you need a moment to consult?

MS. SCOTT: I would appreciate a moment just to make sure I understand the point.

MR. GILLIGAN: Thank you, Your Honor.

(A pause in the proceedings.)

MS. SCOTT: So the final third -- the third point -- he's actually transitioning perfectly to my third point. The third point that they said makes this case different than any other case is that Wikimedia's communications is so ubiquitous, so ubiquitous, a finding on standing could not

harm national security because it wouldn't reveal anything because their communications are everywhere. That's the argument they've made.

They've made that before. And again, he forgot to tell you that in the August 2018 decision, that this Court issued, you already addressed that argument. I'll read from your opinion again.

"Plaintiff contends that, contrary to surveillance of a particular individual with limited communications, plaintiff's communications are so ubiquitous that to reveal surveillance of its communications would not provide information regarding the structure of the Upstream surveillance program or its specific targets.

"Although this proposition may appear to have some force, courts consistently recognized that judicial intuition about this proposition, about -- I apologize, about a proposition such as this, is no substitute for documented risks and threats posed by the potential disclosure of national security."

There the Court quotes *Al Haramain*, a Ninth Circuit decision.

"The defendants have thoroughly documented those risks in the classified declaration here explaining that to reveal the fact of surveillance of an organization such as plaintiff, even considering plaintiff's voluminous online

communications, would provide insight into the structure and operations of Upstream surveillance -- of the Upstream surveillance program. And in so doing undermine the effectiveness of this intelligence method."

Now, that is the case and the Court has already held as such. It is also -- that holding is also directly in line with the Supreme Court's instruction and analysis of the issue from the *Clapper v. Amnesty International* decision in Footnote 4, where it had been suggested in oral argument that the Government could help resolve the issue of standing by disclosing to the Court, perhaps through an in camera proceeding, whether it is intercepting respondent's communications, and what targeting or minimization procedures it is using.

Now, this was not specific to 1806(f), but generally, the Supreme Court said, this type -- said that the suggestion was puzzling to do an ex parte review like this, because as an initial matter it's respondent's burden. Here, it's plaintiff's burden to prove their standing by pointing to specific facts, not the Government's burden to disprove standing by revealing details of its surveillance priorities.

And then the Court continued to discuss how doing such a thing would harm national security by exposing those state secrets privilege types of information to the Court ex parte, and then potentially in its decision later.

Now, the fact that plaintiff's communications are ubiquitous doesn't change that, as this Court has already held.

Now I'd also like to correct another statement that they started with and returned to a few times, which is, they said Dr. Schulzrinne opines about a filter first or put forward a bald hypothetical, I believe is what they said, as to what might be happening. And I'd like to correct that, because Dr. Schulzrinne specifically does not opine on what is more likely here. He doesn't do what Mr. Bradner does, which is speculate about what the NSA may or may not be doing here. He doesn't know. He hasn't been given access to any classified information, just like Mr. Bradner has no access to classified information. And Dr. Schulzrinne cannot say, cannot say how it's mostly done or how it is done, because he doesn't know what the NSA's surveillance practices and priorities and things of -- in this foreign intelligence realm, how they would make decisions because of those things.

What he does, is he says, it could be done via a copy all. It could also technically be done via the filter first mechanism that has many permutations, as he describes: whitelisting, blacklisting, combination.

He doesn't offer an opinion about how it's done because he doesn't know, but he provides us an answer to a very important question: Were they originally correct in

arguing to the Fourth Circuit, to this Court and the Fourth Circuit, that the technical rules of the Internet require that it be done via a copy-all infrastructure. The answer, and now bright blinking lights, is now totally clear because every expert agrees, it can be done multiple ways.

Now, fundamentally this idea that it must be done because of the rules of the Internet only one way, that was plaintiff's argument around or attempted argument around the state secrets privilege. If something can only be done one way, then it can't be a secret, essentially, is what they would argue. Now, we're not conceding that that's the case. You know, maybe it could be done one way and it could still be a secret. But what we have proven here is that factually they're wrong. It could be done multiple ways and how it's done or how it's more likely done, that is a question that the Court cannot step into. And the state secrets doctrine mandates that this Court say they fail to prove their allegation -- sorry, the state secrets privilege doctrine doesn't say -- doesn't mandate that they fail to prove their allegations, but they did. They failed to show a genuine issue in material fact on their allegations, but the state secrets doctrine now demands that it be dismissed, because the central fact they want to litigate, in order to prove standing, is protected by the privilege.

Now --

THE COURT: Anything else?

MS. SCOTT: Yes, Your Honor. With a few more moments of the Court's indulgence, I would like to explain that plaintiffs are wrong when they say that the standard the Court should apply is the substantial risk standard.

Now, in their briefs, they cite for that standard, a Susan B. Anthony List Supreme Court decision.

And I've said, in my opening argument, that *Amnesty International*, the *Clapper v. Amnesty International* decision, is controlling here. And so the correct standard is actual or certainly impending injury.

They think it's substantial risk, but the line of cases that Susan B. Anthony addresses, all show -- all face circumstances where there has been actual action by the Government that can be connected with the plaintiff. So that's a known commodity.

And then, they look to the future injury for that standard.

That is, as the *Clapper* decision held in Footnote 5, that was the wrong standard to apply in *Clapper,* and it's the wrong standard to apply here, because plaintiffs have no proof of actual Government action connected to them specifically.

Moreover, the case they cite for the substantial risk standard, it cites back to *Clapper* and it says, specifically that: The *Amnesty International* plaintiff's

theory of standing, in unifying the two decisions, that case -- plaintiff's theory of standing, was substantially undermined by their failure to offer any evidence that their communications had been monitored under the challenged statute.

So, you know, Susan B. Anthony is not doing anything to disturb the answer that *Clapper* provided, which is that actual action is required and the substantial risks standard is inappropriate. But even more, Footnote 5 in *Clapper* says: Even if the substantial risks standard were applied, in that case, plaintiff's would still fail to meet it because of the chain of attenuated circumstances.

Here, all of this speculation is just such a chain. And this Court should reject that application of the errant -- of the errant standard.

THE COURT: All right. Thank you, Ms. Scott.

All right. The Court will take the matter under advisement. The parties may wish to request a transcript of their arguments from the reporter, presumably your budgets can afford that. I think it might be helpful for the Court to have that. And I'll take the matter under advisement and consider it.

I think the case involves a substantial challenge, let's say, on both sides. And I want to consider it carefully the arguments you've made today and in your briefs. And I

also -- you submitted a good deal of paper in support of it and I want to review that as well.

As usual, the arguments you've made both here and in previous stages of this case have been very helpful and I thank you for it. Court stands in recess.

(Proceedings adjourned at 4:22 p.m.)

CERTIFICATE OF REPORTER

I, Tonia Harris, an Official Court Reporter for the Eastern District of Virginia, do hereby certify that I reported by machine shorthand, in my official capacity, the proceedings had and testimony adduced upon the Remand Hearing in the case of the **WIKIMEDIA FOUNDATION versus NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICES, et al,** Civil Action No. 1:15-CV-662, in said court on the 30th day of May, 2019.

I further certify that the foregoing 69 pages constitute the official transcript of said proceedings, as taken from my machine shorthand notes, my computer realtime display, together with the backup tape recording of said proceedings to the best of my ability.

In witness whereof, I have hereto subscribed my name, this June 7, 2019.

Tonia M. Harris, RPR
Official Court Reporter